Congressional Research Service
Informing the legislative debate since 1914

Terrorism and Security Issues Facing the Water Infrastructure Sector

Updated November 28, 2012

Congressional Research Service
https://crsreports.congress.gov
RL32189

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Damage to or destruction of the nation's water supply and water quality infrastructure by terrorist attack or natural disaster could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life. Interest in such problems increased after the September 11, 2001, terrorist attacks in the United States.

Across the country, water infrastructure systems extend over vast areas, and ownership and operation responsibility are both public and private, but are overwhelmingly non-federal. Since the attacks, federal dam operators and local water and wastewater utilities have been under heightened security conditions and are evaluating security plans and measures. There are no federal standards or agreed-upon industry practices within the water infrastructure sector to govern readiness, response to security incidents, and recovery. Efforts to develop protocols and tools are ongoing since the 9/11 terrorist attacks. This report presents an overview of this large and diverse sector, describes security-related actions by the government and private sector since 9/11, and discusses additional policy issues and responses, including congressional interest.

Policymakers have been considering a number of initiatives, including enhanced physical security, better communication and coordination, and research. A key issue is how additional protections and resources directed at public and private sector priorities will be funded. In response, Congress has provided some appropriations for security at water infrastructure facilities (to assess and protect federal facilities and support security assessment and risk reduction activities by non-federal facilities) and passed a bill requiring drinking water utilities to conduct security vulnerability assessments (P.L. 107-188). When Congress created the Department of Homeland Security (DHS) in 2002 (P.L. 107-297), it gave DHS responsibilities to coordinate information to secure the nation's critical infrastructure, including the water sector. Under Homeland Security Presidential Directive-7, the Environmental Protection Agency (EPA) is the lead federal agency for protecting drinking water and wastewater utility systems.

Recent congressional interest has focused on two legislative issues: (1) security of wastewater utilities, and (2) whether to include water utilities in chemical plant security regulations implemented by DHS. Congress has considered legislation to encourage wastewater treatment works to conduct vulnerability assessments and develop site security plans, but none has been enacted. Congress also has considered legislation to extend DHS's Chemical Facilities Anti-Terrorism Standards and, as part of that debate, whether to preserve an existing exemption for water utilities from chemical facility standards or to include them in the scope of DHS security rules. For now, the exemption from DHS standards remains in place.

Since the terrorist attacks of 2001, wastewater and drinking water utilities have been engaged in numerous activities to assess potential vulnerabilities and strengthen facility and system protections. Congressional oversight of this sector's homeland security activities has been limited but could be of interest in the 113th Congress.

Contents

Contacts

Introduction

The September 11, 2001, attacks on the World Trade Center and the Pentagon have drawn attention to the security of many institutions, facilities, and systems in the United States, including the nation's water supply and water quality infrastructure. These systems have long been recognized as being potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism/chemical contamination, and cyber attack. Damage or destruction by terrorist attack could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life. Further, since most water infrastructure is government-owned, it may serve as a symbolic and political target for some. This report presents an overview of this large and diverse sector, describes security-related actions by the government and private sector since 9/11, and discusses additional policy issues and responses, including congressional interest.

The potential for terrorism is not new. In 1941, Federal Bureau of Investigation Director J. Edgar Hoover wrote, "It has long been recognized that among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace."[1] Water infrastructure systems also are highly linked with other infrastructure systems, especially electric power and transportation, as well as the chemical industry which supplies treatment chemicals, making security of all of them an issue of concern. These types of vulnerable interconnections were evident, for example, during the August 2003 electricity blackout in the Northeast United States: wastewater treatment plants in Cleveland, Detroit, New York, and other locations that lacked backup generation systems lost power and discharged millions of gallons of untreated sewage during the emergency, and power failures at drinking water plants led to boil-water advisories in many communities. Likewise, natural disasters such as the 2005 Gulf Coast hurricanes and 2007 Mississippi River floods caused extensive and costly damage to multiple infrastructure systems—transportation, water, electric power, and telecommunications.

Background

Broadly speaking, water infrastructure systems include surface and ground water sources of untreated water for municipal, industrial, agricultural, and household needs; dams, reservoirs, aqueducts, and pipes that contain and transport raw water; treatment facilities that remove contaminants from raw water; finished water reservoirs; systems that distribute water to users; and wastewater collection and treatment facilities. Across the country, these systems comprise approximately 77,000 dams and reservoirs; thousands of miles of pipes, aqueducts, water distribution, and sewer lines; 168,000 public drinking water facilities (many serving as few as 25 customers); and about 16,000 publicly owned wastewater treatment facilities. All of these systems and facilities must be operable 24 hours a day, seven days a week. Ownership and management are both public and private; the federal government has ownership responsibility for hundreds of dams and diversion structures, but the vast majority of the nation's water infrastructure is either privately owned or owned by non-federal units of government.

The federal government has built hundreds of water projects, primarily dams and reservoirs for irrigation development and flood control, with municipal and industrial water use as an

[1] J.E. Hoover, "Water Supply Facilities and National Defense," *Journal of the American Water Works Association,* vol. 33, no. 11 (1941), 1861.

incidental, self-financed, project purpose. Many of these facilities are critically entwined with the nation's overall water supply, transportation, and electricity infrastructure. The largest federal facilities were built and are managed by the Bureau of Reclamation (Reclamation) of the Department of the Interior and the U.S. Army Corps of Engineers (Corps) of the Department of Defense.

Reclamation reservoirs, particularly those along the Colorado River, supply water to millions of people in southern California, Arizona, and Nevada via Reclamation and non-Reclamation aqueducts. Reclamation's inventory of assets includes 471 dams and dikes that create 348 reservoirs with a total storage capacity of 245 million acre-feet of water. Reclamation projects also supply water to 9 million acres of farmland and other municipal and industrial water users in the 17 western states. The Corps operates 276 navigation locks, 11,000 miles of commercial navigation channel, and approximately 1,200 projects of varying types, including 609 dams. It supplies water to thousands of cities, towns, and industries from the 9.5 million acre-feet of water stored in its 116 lakes and reservoirs throughout the country, including service to approximately 1 million residents of the District of Columbia and portions of northern Virginia.

The largest Corps and Reclamation facilities also produce enormous amounts of power. For example, Hoover and Glen Canyon dams on the Colorado River represent 23% of the installed electrical capacity of the Bureau of Reclamation's 58 power plants in the West and 7% of the total installed capacity in the Western United States. Similarly, Corps facilities and Reclamation's Grand Coulee Dam on the Columbia River provide 43% of the total installed hydroelectric capacity in the West (25% nationwide). Still, despite its critical involvement in such projects, especially in the West, the federal government is responsible for only about 5% of the dams whose failure could result in loss of life or significant property damage. The remaining dams belong to state or local governments, utilities, and corporate or private owners.

A fairly small number of large drinking water and wastewater utilities located primarily in urban areas (about 15% of the systems) provide water services to more than 75% of the U.S. population. Arguably, these systems represent the greatest targets of opportunity for terrorist attacks, while the larger number of small systems that each serve fewer than 10,000 persons are less likely to be perceived as key targets by terrorists who might seek to disrupt water infrastructure systems. However, the more numerous smaller systems also tend to be less protected and, thus, are potentially more vulnerable to attack, whether by vandals or terrorists. A successful attack on even a small system could cause widespread panic, economic impacts, and a loss of public confidence in water supply systems.

Attacks resulting in physical destruction to any of these systems could include disruption of operating or distribution system components, power or telecommunications systems, electronic control systems, and actual damage to reservoirs and pumping stations. A loss of flow and pressure would cause problems for customers and would hinder firefighting efforts. Further, destruction of a large dam could result in catastrophic flooding and loss of life. Bioterrorism or chemical attacks could deliver widespread contamination with small amounts of microbiological agents or toxic chemicals, and could endanger the public health of thousands. While some experts believe that risks to water systems actually are small, because it would be difficult to introduce sufficient quantities of agents to cause widespread harm, concern and heightened awareness of potential problems are apparent. Factors that are relevant to a biological agent's potential as a weapon include its stability in a drinking water system, virulence, culturability in the quantity required, and resistance to detection and treatment. Cyber attacks on computer operations can affect an entire infrastructure network, and hacking in water utility systems could result in theft or corruption of information, or denial and disruption of service.

Responses to Security Concerns

Water infrastructure system designers, managers, and operators have long made preparing for extreme events a standard practice. Historically, their focus has been on natural events—major storms, blizzards, and earthquakes—some of which could be predicted hours or longer before they occurred. When considering the risk of manmade threats, operators generally focused on purposeful acts such as vandalism or theft by disgruntled employees or customers, rather than broader malevolent threats by terrorists, domestic or foreign. The events of September 11, 2001, changed this focus.

Federal dam operators went on "high-alert" immediately following the 9/11 terrorist attacks. Reclamation closed its visitor facilities at Grand Coulee, Hoover, and Glen Canyon dams. Because of potential loss of life and property downstream if breached, security threats are under constant review, and coordination efforts with both the National Guard and local law enforcement officials are ongoing. The Corps temporarily closed all its facilities to visitors immediately after 9/11, although locks and dams remained operational; most closed facilities later re-opened, but security continues to be reassessed. Following a heightened alert issued by the federal government in February 2003, Reclamation implemented additional security measures which remain in effect at dams, powerplants, and other facilities, including limited access to facilities and roads, closure of some visitor centers, and random vehicle inspections.

Although officials believe that risks to water and wastewater utilities are small, operators have been under heightened security conditions since 9/11. Local utilities have primary responsibility to assess their vulnerabilities and prioritize them for necessary security improvements. Most (especially in urban areas) have emergency preparedness plans that address issues such as redundancy of operations, public notification, and coordination with law enforcement and emergency response officials. However, many plans were developed to respond to natural disasters, domestic threats such as vandalism, and, in some cases, cyber attacks. Drinking water and wastewater utilities coordinated efforts to prepare for possible Y2K impacts on their computer systems on January 1, 2000, but these efforts focused more on cyber security than physical terrorism concerns. Thus, it was unclear whether previously existing plans incorporate sufficient procedures to address other types of terrorist threats. Utility officials are reluctant to disclose details of their systems or these confidential plans, since doing so might alert terrorists to vulnerabilities.

Water supply was one of eight critical infrastructure systems identified in President Clinton's 1998 Presidential Decision Directive 63 (PDD-63)[2] as part of a coordinated national effort to achieve the capability to protect the nation's critical infrastructure from intentional acts that would diminish them. These efforts focused primarily on the 340 large community water supply systems which each serve more than 100,000 persons. The Environmental Protection Agency (EPA) was identified as the lead federal agency for liaison with the water supply sector. In response, in 2000, EPA established a partnership with the American Metropolitan Water Association (AMWA) and American Water Works Association (AWWA) to jointly undertake measures to safeguard water supplies from terrorist acts. AWWA's Research Foundation contracted with the Department of Energy's Sandia National Laboratory to develop a vulnerability assessment tool for water systems (as an extension of methodology for assessing federal dams). EPA supported a project with the Sandia Lab to pilot test the physical vulnerability assessment tool and develop a cyber vulnerability assessment tool. An Information Sharing and

[2] "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998; see http://www.fas.org/irp/offdocs/paper598.htm.

Analysis Center (ISAC) supported by an EPA grant became operational under AMWA's leadership in December 2002. It allows for dissemination of alerts to drinking water and wastewater utilities about potential threats or vulnerabilities to the integrity of their operations that have been detected and viable resolutions to problems.[3]

Research on water sector infrastructure protection has been underway for some time. The Department of the Army conducts research in the area of detection and treatment to remove various chemical agents. The Federal Emergency Management Agency (FEMA) has led an effort to produce databases of water distribution systems and to develop assessment tools for evaluating threats posed by the introduction of a biological or chemical agent into a water system. The Centers for Disease Control and Prevention is developing guidance on potential biological agents and the effects of standard water treatment practices on their persistence. However, in the 2001 report of the President's Commission on Critical Infrastructure Protection, ongoing water sector research was then characterized as a small effort that leaves a number of gaps and shortfalls relative to U.S. water supplies.[4] This report stated that gaps exist in four major areas, concerns that remain relevant and continue to guide policymakers.

- Threat/vulnerability risk assessments,
- Identification and characterization of biological and chemical agents,
- A need to establish a center of excellence to support communities in conducting vulnerability and risk assessment, and
- Application of information assurance techniques to computerized systems used by water utilities, as well as the oil, gas, and electric sectors, for operational data and control operations.

For some time, less attention was focused on protecting wastewater treatment facilities than drinking water systems, perhaps because destruction of them likely represents more of an environmental threat (i.e., by release of untreated sewage) than a direct threat to life or public welfare. Vulnerabilities do exist, however. Large underground collector sewers could be accessed by terrorist groups for purposes of placing destructive devices beneath buildings or city streets. Pipelines can be made into weapons via the introduction of a highly flammable substance such as gasoline through a manhole or inlet. Explosions in the sewers can cause collapse of roads, sidewalks, and adjacent structures and injure and kill people nearby. Damage to a wastewater facility prevents water from being treated and can impact downriver water intakes. Destruction of containers that hold large amounts of chemicals at treatment plants could result in release of toxic chemical agents, such as chlorine gas, which can be deadly to humans if inhaled and, at lower doses, can burn eyes and skin and inflame the lungs.

Since the 2001 terrorist attacks, many water and wastewater utilities have switched from using chlorine gas as disinfection to alternatives which are believed to be safer, such as sodium hypochlorite or ultraviolet light. However, some consumer groups remain concerned that many wastewater utilities, including facilities that serve heavily populated areas, continue to use chlorine gas. To prepare for potential accidental releases of hazardous chemicals from their facilities, more than 2,800 wastewater and drinking water utilities, water supply systems, and irrigation systems already are subject to risk management planning requirements under the Clean

[3] For additional information, see http://www.waterisac.org/.

[4] Critical Infrastructure Assurance Office, *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities,* January 2001, 209 p. See http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf.

Air Act. Still, some observers advocate requiring federal standards to ensure that facilities using dangerous chemicals, such as wastewater treatment plants, use the best possible industry practices (practices that are referred to as Inherently Safer Technologies, or ISTs) to reduce hazards.[5] In 2007, the U.S. Chemical Safety and Hazard Investigation Board issued a safety bulletin recommending that the Department of Transportation increase regulation of wastewater and drinking water treatment plants and other types of facilities that receive chlorine gas by railcar to require that they install remotely operated emergency isolation devices to unload chlorine railcars, for rapid shutdown in the event of leakage or other failure.[6]

In 2006, the Government Accountability Office (GAO) reported on a survey of security measures at 200 of the nation's largest wastewater utilities.[7] GAO found that many have made security improvements since the 2001 terrorist attacks. Most utilities said they had completed, or intended to complete, a plan to conduct some type of security assessment, although there is no federal mandate to do so. More than half of responding facilities indicated they did not use potentially dangerous gaseous chlorine as a wastewater disinfectant. However, the report noted that these utilities have made little effort to address collection system vulnerabilities, due to the technical complexity and expense of securing collection systems that cover large areas and have many access points. Some told GAO investigators that taking other measures, such as converting from gaseous chlorine, took priority over collection system protections. In a 2007 follow-on study, GAO reported that actual and projected capital costs to convert from chlorine gas to alternative disinfection methods range from about $650,000 to just over $13 million. Factors affecting conversion costs included the type of alternative method; the size of the facility; and labor, building, and supply costs, which varied considerably.[8]

There are no federal standards or agreed-upon practices within the water infrastructure sector to govern readiness, response to security incidents, and recovery. EPA is not authorized to require water infrastructure systems to implement specific security improvements or meet particular security standards. Efforts to develop voluntary protocols and tools are ongoing since the 2001 terrorist attacks. Wastewater and drinking water utility organizations are implementing computer software and training materials to evaluate vulnerabilities at large, medium, and small utility systems, and EPA has provided some grant assistance to drinking water utilities for vulnerability assessments. Out of funds appropriated in 2002 (P.L. 107-117), EPA awarded grants to nearly 900 large and medium drinking water utilities to conduct vulnerability assessments. EPA also has targeted grants to "train the trainers," delivering technical assistance to organizations such as the Rural Community Assistance Program and the Water Environment Federation that, in turn, can assist and train personnel at thousands of medium and small utilities throughout the country. Rural and small systems also have received support from the U.S. Department of Agriculture.

With financial support from EPA, drinking water and wastewater utility and engineering groups developed three security guidance documents, issued in 2004, that cover the physical design of

[5] See, for example, Environmental Defense, *Eliminating Hometown Hazards, Cutting Chemical Risks at Wastewater Treatment Facilities,* December 2003, 14 p.; and Center for American Progress, *Toxic Trains and the Terrorist Threat, How Water Utilities Can Get Chlorine Gas Off the Rails and Out of American Communities,* April 2007, 23 p.

[6] For information, see http://www.chemsafety.gov/index.cfm?folder=recommendations.

&page=details&ReportID=40&RecipientID=78&show=yes#78.

[7] U.S. Government Accountability Office, *Securing Wastewater Facilities, Utilities Have Made Important Upgrades but Further Improvements to Key System Components May Be Limited by Costs and Other Constraints,* GAO-06-390, March 2006, 64 p.

[8] U.S. Government Accountability Office, *Securing Wastewater Facilities, Costs of Vulnerability Assessments, Risk Management Plans, and Alternative Disinfection Methods Vary Widely*, GAO-07-480, March 2007, 26 p.

online contaminant monitoring systems, and physical security enhancements of drinking water, wastewater, and stormwater infrastructure systems. The documents provide voluntary guidelines for assisting utilities that have completed vulnerability assessments to mitigate vulnerabilities of their systems through the design, construction, operation, and maintenance of both new and existing systems. Based on the three guidance documents, these groups also have drafted training materials and a set of voluntary standardized best engineering practices that recommend measures to protect water and wastewater infrastructure against a range of threats, including terrorist attacks and other sources of potential harm, such as accidents, chemical contamination, and natural disasters.[9]

EPA

EPA has taken a number of organizational and planning steps to strengthen water security. The agency created a National Homeland Security Research Center within the Office of Research and Development to develop the scientific foundations and tools that can be used to respond to attacks on water systems. The Center conducts applied research on ways to protect and prevent, mitigate, respond to, and recover from security events. EPA also created a Water Security Division in the Office of Water, taking over activities initiated by a Water Protection Task Force after the 9/11 terrorist attacks. This office provides guidance and tools to utilities as they assess and reduce vulnerabilities of their systems. It trains water utility personnel on security issues, supports the WaterISAC, and implements the agency's comprehensive research plan.

In 2004 EPA issued a Water Security Research and Technical Support Action Plan, identifying critical research needs and providing an implementation plan for addressing those needs. A preliminary review of the Research and Action Plan by a panel of the National Research Council identified some gaps, suggested alternative priorities, and noted that the Plan was silent on the financial resources required to complete the research and to implement needed countermeasures to improve water security. Subsequently, in 2007, the National Research Council concluded that EPA has developed useful contaminant information and exposure assessment tools in several key areas, but that other areas, such as physical and cyber security, contingency planning, and wastewater security, have shown weaker or somewhat disjointed progress. An overarching issue is making water security information accessible to those who might need it.[10]

GAO has issued two reports discussing how future federal funding can best be spent to improve security at drinking water and wastewater utilities.[11] Both reports are based on the views of subject matter experts identified by GAO. In the drinking water report, specific activities judged by the experts to be most deserving of federal support included physical and technological upgrades, education and training for staff and responders, and strengthening key relationships between water utilities and others such as law enforcement and public health agencies. In the wastewater report, the experts cited the replacement of gaseous chemicals used in the disinfection process with less hazardous alternatives as a key activity deserving of federal funds, along with improving local, state, and regional collaboration, and support facilities' vulnerability assessments. Asked how federal funds should be allocated, both groups of experts favored giving

[9] See http://www.asce.org/static/1/wise.cfm.

[10] National Academies Press, *Improving the Nation's Water Security, Opportunities for Research,* Water Science and Technology Board, 2007. Hereafter, *Improving the Nation's Water Security.*

[11] U.S. Government Accountability Office, *Drinking Water, Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*, GAO-04-29, October 2003, 69 p.; and *Wastewater Facilities, Experts' Views on How Federal Funds Should Be Spent to Improve Security*, GAO-05-165, January 2005, 70 p.

priority to utilities that serve critical assets (such as public health institutions, government, and military bases) and to utilities serving areas with large populations.

A key focus of EPA's activities since 2005 has been the Water Sector Initiative. Initially known as WaterSentinel, it is a pilot project that could serve as a model for water utilities throughout the country. Its purpose is to test and demonstrate contamination warning systems at drinking water utilities and municipalities. EPA awarded grants to install and evaluate early warning systems in five cities under this program (Cincinnati, New York, San Francisco, Dallas, and Philadelphia).

More broadly, EPA has expanded its security activities in two ways. First, its focus has enlarged from the post-9/11 emphasis on terrorism to an "all hazards" approach, emphasizing to water utilities that issues of risk identification and risk reduction also include natural disasters (which were the focus of much of the industry's attention before 2001) and protection of hazardous chemicals. Second, EPA supports the establishment of intrastate mutual aid and assistance agreements, known as Water/Wastewater Agency Response Networks (WARNS), to facilitate flow of personnel and resources during response to emergencies. They are intended to provide mechanisms for establishing emergency contacts and facilitating short-term emergency assistance to restore critical operations. Mutual aid agreements existed in California and Florida before the 2005 Gulf hurricanes, and more formal efforts to establish similar programs in all 50 states followed on those disasters. So far, WARNS have been established in about 20 states, according to EPA.

The agency also has developed a variety of guidance documents and other information resources to support drinking water and wastewater utility preparedness, response, and recovery.[12]

- A Vulnerability Self-Assessment Tool (VSAT), a risk assessment software tool to assist drinking water and wastewater owners and operators in performing security threats and natural hazards risk assessments, as well as updating emergency response plans.
- A Water Contaminant Information Tool (WCIT), a secure online database with information for federal, state, and local agencies and emergency responders about chemical, biological, and radiochemical contaminants of concern for the water sector.
- A scenario-based Tabletop Exercise Tool for Water Systems (TTX Tool) that addresses emergency preparedness and response for a number of potential natural hazards and manmade incidents.
- A Water Health and Economic Analysis Tool (WHEAT) to assist drinking water utilities in quantifying public health impacts, utility financial costs, and regional economic impacts of an adverse event. Currently this two examines two scenarios: release of hazardous gas, or loss of operating assets in a drinking water distribution system.

Reclamation and the Corps

Officials have been reassessing federal infrastructure status and vulnerabilities for several years.[13] The Bureau of Reclamation's site security program is aimed at ensuring protection of Reclamation's 252 high- and significant-hazard dams and facilities and 58 hydroelectric plants.

[12] For information, see http://www.epa.gov/infrastructure/watersecurity/index.cfm.

[13] For additional information, see CRS Report RL34466, *The Bureau of Reclamation's Aging Infrastructure*, by Charles V. Stern.

After September 11, Reclamation committed to conducting vulnerability and risk assessments at 280 high-priority facilities. Risk assessments at these facilities were completed between FY2002 and FY2006. These assessments resulted in recommendations now being implemented to enhance security procedures and physical facilities, such as additional security staffing, limited vehicle and visitor access, and coordination with local law enforcement agencies. The Corps implements a facility protection program to detect, protect, and respond to threats to Corps facilities and a dam security program to coordinate security systems for Corps infrastructure. It also implements a national emergency preparedness program which assists civilian governments in responding to all regional/national emergencies, including acts of terrorism. Both agencies participate in the Interagency Committee on Dam Safety (ICODS), which is part of the National Dam Safety Program that is led by FEMA.

A 2003 White House report[14] presented a national strategy for protecting the nation's critical infrastructures and identified four water sector initiatives: identify high-priority vulnerabilities and improve site security; improve monitoring and analytic capabilities; improve information exchange and coordinate contingency planning; and work with other sectors to manage unique risks resulting from interdependencies. The strategy was intended to focus national protection priorities, inform resource allocation processes, and be the basis for cooperative public and private protection actions.

Department of Homeland Security

The Department of Homeland Security (DHS, established in P.L. 107-297) has a mandate to coordinate securing the nation's critical infrastructure, including water infrastructure, through partnerships with the public and private sectors. It is responsible for detailed implementation of core elements of the national strategy for protection of critical infrastructures. One of its tasks is to assess infrastructure vulnerabilities, an activity that wastewater and drinking water utilities have been doing since the 9/11 attacks, under their own initiatives and congressional mandates (P.L. 107-188; see "Legislative Issues").The legislative reorganization did not transfer Corps or Reclamation responsibilities for security protection of dams and other facilities or EPA's responsibilities to assist drinking water and wastewater utilities.

In 2003, President Bush issued Homeland Security Presidential Directive/HSPD-7 which established a national policy for the federal government to identify, prioritize, and protect critical infrastructure as a part of homeland security.[15] The directive called for DHS to integrate all security efforts among federal agencies and to complete a comprehensive national plan for critical infrastructure protection. In 2006, DHS issued a National Infrastructure Protection Plan (NIPP), proposing a framework of partnerships between private industry sectors and the government that would work together to secure the nation's vital resources. For example, EPA would work with water treatment and wastewater systems, while dams would cooperate with DHS. The Department updated the NIPP in February 2009.[16] The plan is intended to provide the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation's critical infrastructure and key resources into a single national program.

---

[14] The White House, Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, 90 p.

[15] The White House, *December 17, 2003 Homeland Security Presidential Directive/ HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection.* HSPD-7 superseded PDD-63, which started the process of federal protection of critical infrastructure even before the 2001 terrorist attacks.

[16] U.S. Department of Homeland Security, *National Infrastructure Protection Plan 2009*, February 2009, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

The Department established the Critical Infrastructure Partnership Advisory Council (CIPAC) to coordinate federal infrastructure protection programs with similar activities of the private sector, and state, local, and tribal governments. In 2004, CIPAC established a Government Coordinating Council (GCC) and non-government coordinating council for each sector. The CIPAC Water Sector Committee includes representatives from both the Water GCC (federal members) and the Water Sector Coordinating Council (WSCC). The WSCC consists of 24 members from state and local agencies, water utilities, and water affinity organizations.

In response to the original NIPP, DHS and the GCCs, in conjunction with the Sector Coordinating Councils, prepared 17 sector-specific plans which were completed in 2007. The plans identify sector profiles and assets, assess risks, prioritize infrastructure, identify sector protection plans and measures of progress. The water sector plan for wastewater and drinking water focuses on four goals: (1) sustaining protection of public health and the environment; (2) recognize and reduce risks; (3) maintain a resilient infrastructure; and (4) increase communication, outreach, and public confidence.[17] The sector plan for dams, including federal dams, is one of 10 that DHS determined presents security sensitivity issues if widely distributed; thus, those 10 plans were not released to the public. In an early review of the sector plans, GAO found that the drinking water and wastewater sector plan was more developed than that of many other sectors, largely because the sector has a 30-year history of protection and cooperation, but for that reason, the plan did not provide added value for the sector.[18]

In the NIPP, DHS described a plan to develop a risk analysis method that would include a uniform means of measuring risk and assessing consequences across infrastructure sectors. Some drinking water and wastewater treatment industry officials commented that this plan, known as the Risk Analysis and Management for Critical Asset Protection (RAMCAP), raised concern that it could force some facilities to conduct new, or revise existing, vulnerability assessments. Drinking water industry officials are said to be concerned that a new method may not recognize vulnerability assessments that many drinking water utilities have already completed under requirements of the 2002 Bioterrorism Preparedness Act (see "Legislative Issues"). This is a particular concern for small and rural utilities, many of which have used simpler security models to complete their vulnerability assessment plans and would prefer to build on that model to conduct RAMCAP and similar activities.

While physical security of facilities is a key concern, cyber security issues continue to draw attention, as well. The Water Sector Coordinating Council has developed guidance on protecting potentially vulnerable drinking water and wastewater systems from targeted cyber attack or accidental cyber events and has hosted workshops for utility employees who are responsible for control system security.[19]

Coordination and Information Sharing

The Homeland Security Department's involvement in water security concerns has been growing, although under HSPD-7, EPA continues as the lead federal agency to ensure protection of drinking water and wastewater treatment systems from possible terrorist acts and other sabotage.

[17] U.S. Department of Homeland Security and U.S. Environmental Protection Agency, Water, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, May 2007, 122 p. See http://www.dhs.gov/xlibrary/assets/Water_SSP_5_21_07.pdf.

[18] U.S. Government Accountability Office, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve,* GAO-07-706R, July 10, 2007, p. 4.

[19] Water Sector Coordinating Council Cyber Security Working Group, *Roadmap to Secure Control Systems in the Water Sector*, March 2008, http://www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf.

Since early 2004, DHS has been preparing guidance documents on how each infrastructure sector, including water systems, can protect itself from security threats. For some time, the two agencies have been working to clarify their roles in providing security to water utilities.

One of the functions of the Water Sector Coordinating Council is to be a point of contact for DHS to vet potential water security policies, allowing one-stop shopping for federal officials. In 2003, DHS created an information-sharing network, called the Homeland Security Information Network (HSIN). Both it and the existing WaterISAC share the goal of providing security information to water utilities, but they differ in some respects. The WaterISAC is a private, subscription service (although it receives some federal funding) that provides information to about 450 water utilities and others on security matters. It is the primary communication tool in the water sector. The HSIN, a software program, is a free, federally funded platform for information sharing. It is not limited to the water sector, and it provides no information by itself; it acts as a bulletin board where DHS, EPA, and utilities can post security-related information. Distinct from the HSIN and the WaterISAC is the Water Security Channel (WaterSC), launched in 2004 as a free service of the WaterISAC, which disseminates EPA and DHS general security bulletins at the request of those agencies to more than 8,400 utilities, state agencies, engineering firms, and researchers.

Policy Issues

Congress and other policymakers have considered a number of initiatives in this area, including enhanced physical security, communication and coordination, and research. Regarding physical security, a key question is whether protective measures should be focused on the largest water systems and facilities, where risks to the public are greatest, or on all, since small facilities may be more vulnerable. A related question is responsibility for additional steps, because the federal government has direct control over only a limited portion of the water infrastructure sector. The distributed and diverse nature of ownership (federal, non-federal government, and private) complicates assessing and managing risks, as does the reality of limited resources. The adequacy of physical and operational security safeguards is an issue for all in this sector. One possible option for federal facilities (dams and reservoirs maintained by Reclamation and the Corps) is to restrict visitor access, including at adjacent recreational facilities, although such actions could raise objections from the public. Some operators of non-federal facilities and utilities are likewise concerned. As a precaution after the 9/11 attacks, New York City, which provides water to 9 million consumers, closed its reservoirs indefinitely to all fishing, hiking, and boating and blocked access to some roads.

Policymakers have examined measures that could improve coordination and exchange of information on vulnerabilities, risks, threats, and responses. This is a key objective of the WaterISAC and also of the Department of Homeland Security, which includes, for example, functions of the National Infrastructure Protection Center (NIPC) of the FBI that brings together the private sector and government agencies at all levels to protect critical infrastructure, especially on cyber issues. One issue of interest is how the Department is coordinating its activities with ongoing security efforts by other federal agencies and non-federal entities that operate water infrastructure systems, including its implementation of the comprehensive national plan required by Presidential Directive/HSPD-7.

For some time, the two agencies have been working to clarify their roles in providing security to water utilities and in other areas and have negotiated agreements concerning joint research projects and coordination for specific field operations. Nevertheless, in the conference report accompanying the FY2005 Consolidated Appropriations Act, Congress directed EPA to enter into a memorandum of understanding (MOU) with DHS to define the relationship of the two entities

with regard to the protection and security of the nation. The memorandum was expected to specifically identify areas of responsibilities and the potential costs (including which entity pays, in whole or part) for meeting such responsibilities.[20] EPA responded to this directive in November 2005 by issuing a report that identified general authorities that govern EPA's and DHS's respective actions, ongoing projects that reflect coordination, and existing project-specific MOUs.

This EPA report on roles and responsibilities still may not resolve the potential for duplication and overlap among agencies. Currently, for example, policies are being developed both by DHS and EPA, although both agencies are represented on DHS's Water Sector Committee through the CIPAC process. Information sharing and dissemination even in this one sector are occurring through several different mechanisms: DHS supports the Homeland Security Information Network (HSIN), while drinking water and wastewater utilities also may receive security-related advisories from two other sources, the WaterISAC and the Water Security Channel. Some have questioned the multiple advisory groups, on top of existing entities, and in particular the potential that the several mechanisms for sharing homeland security information could transmit inconsistent information and make the exchange of information more complicated, not less. Others are optimistic that the systems and groups will sort themselves out into compatible and complementary networks of information sharing, but that process could take considerable time.

In its March 2006 report, GAO commented on these multiple information services designed to communicate information to the water sector, but also acknowledged EPA's and DHS's ongoing efforts to coordinate their activities to advance water sector security. GAO recommended that DHS and the Water Sector Coordinating Council identify areas where information-sharing networks supported by EPA and DHS (especially the WaterISAC and HSIN) could be better coordinated to avoid operational duplications and overlap and to ensure that security threat information is provided to water systems on a timely basis. Water utility industry groups responded to GAO's recommendation by saying that such coordination efforts are, in fact, underway.

DHS-EPA coordination again received congressional attention in the 110th Congress. In its draft report on FY2009 funding for DHS, the House Appropriations Committee included report language urging DHS to work with EPA on water security issues. The report encouraged the National Protection and Programs Directorate of DHS to work with EPA "to improve federal outreach to water system managers, increase support and guidance on implementation of risk assessment techniques, and publicize effective protective measures that can be taken to increase water system security."[21]

Beyond the water sector itself, there is interest in larger coordination issues involving cross-sector interdependencies of critical infrastructures. As noted previously, water utilities are dependent on electric power to treat and distribute power, and electric power is essential to collecting and treating wastewater. Adequate and uninterrupted supply of water is necessary to support municipal firefighting.[22] When disasters occur, what affects power also affects water supply, also affects sanitary services, also affects communications capability. The National Infrastructure Advisory Council, which provides the President, through DHS, with advice on infrastructure security, reportedly is currently engaged in a regional resilience study focused on the Philadelphia

[20] H.Rept. 108-792, to accompany H.R. 4818, Consolidated Appropriations Act, 2005, *Congressional Record*, daily edition, November 19, 2004, p. H10850.

[21] U.S. Congress, House, Committee on Appropriations, "Draft report to accompany Department of Homeland Security Appropriations Bill, 2009," 110th Congress, 2d session, p. 97.

[22] *Improving the Nation's Water Security*, p. 10.

region that is examining interdependencies of water and other critical sectors (e.g., energy, telecommunications, transportation).

Another information issue concerns the extent of EPA's ability to collect and analyze security data from water utilities, especially information in vulnerability assessments submitted under the Bioterrorism Preparedness Act (discussed below). EPA officials believe that the act permits reviewing utility submissions for overall compliance and allows aggregation of data but precludes the agency from asking for or analyzing data showing changes in security levels, as a safeguard against unintended release of such information. Others, including EPA's Inspector General, believe that EPA has the authority and responsibility to review and analyze the information in order to identify and prioritize threats and to develop plans to protect drinking water supplies.

Among the research needs being addressed real-time monitoring of water supplies, and development of information technology. The cost of additional protections and how to pay for them are issues of great interest, and policymakers continue to consider resource needs and how to direct them at public and private sector priorities. A critical issue for drinking water and wastewater utilities is how to pay for physical security improvements, since currently there are no federal funds dedicated to these purposes, and utilities generally must pay for improvements using the same revenue or funding sources also needed for other types of capital projects.

Congressional Response

Since the September 11, 2001 attacks, Congress has conducted oversight on a number of these issues and considered legislation to address various policy issues, including government reorganization, and additional appropriations.

Appropriations

Since the 9/11 terrorist attacks, Congress has provided appropriations to the Corps, the Bureau, and EPA for security-related programs and activities to protect water infrastructure.

For both the Bureau of Reclamation and the Army Corps of Engineers, appropriations immediately after 9/11 were intended to support risk assessment of needed security improvements, followed by implementation of measures to ensure the safety and security of the public, Reclamation and Corps employees, and the facilities. For example, since FY2004, both agencies have implemented physical hardening and other protective measures, as well as personnel and information security. Both agencies continue to assess and reassess security needs at their facilities as part of ongoing efforts to ensure their long-term security. Reclamation's security budget includes a law enforcement program (guards and surveillance), facility fortification, studies, and review. For several years, Reclamation's security activities focused on five National Critical Infrastructure (NCI) dam facilities: Hoover, Shasta, Grand Coulee, Glen Canyon, and Fulsom; in recent years, other facilities also have received recommended security upgrades. Physical security enhancements at Reclamation facilities are intended to protect those facilities from terrorist threats, other criminal activities, and unauthorized operation of water control systems, thus reducing the high risk rating at critical assets. Several independent and internal reviews were conduction of Reclamation's site security program (including a review by Sandia National Laboratory, Interior's Office of Inspector General, and the National Academy of Sciences). As a result, Reclamation implemented improvements to all components of its program, including personnel security, information security, facility security, operations security, and law enforcement.

The Corps' budget covers recurring security costs (i.e., guards and monitoring) for its administrative buildings and other general use facilities. The Corps also funds certain project-specific facility security upgrades.

Funding appropriated to EPA has supported a number of activities. Significant portions of appropriations in FY2002 and FY2003 were for EPA grants for vulnerability assessments carried out by large and medium-size drinking water systems, to assist them in complying with requirements of the Public Health Security and Bioterrorism Preparedness and Response Act (P.L. 107-188, discussed below). EPA appropriations also supported training and development of voluntary industry practices for security, and grants to states and territories to coordinate activities for critical water infrastructure security efforts.[23] EPA also provides support for water security information sharing for drinking water and wastewater utilities through the WaterISAC and the Water Security Channel. EPA has supported two special initiatives since FY2006: the Water Alliance for Threat Reduction (WATR), to train utility operators at the highest risk systems; and a related pilot program, the Water Sector Initiative, to design, deploy, and test biological or other contamination warning systems at drinking water.

Legislative Issues

In May 2002, Congress approved the Public Health Security and Bioterrorism Preparedness and Response Act (P.L. 107-188). Title IV of that act required drinking water systems serving more than 3,300 persons to conduct vulnerability analyses and to submit the assessments to EPA. The legislation authorized grant funding to assist utilities in meeting these requirements.[24] Legislation authorizing Reclamation to contract with local law enforcement to protect its facilities also was enacted during the 107th Congress (P.L. 107-69).

In 2001, the House and Senate considered but did not enact legislation authorizing a six-year grant program for research and development on security of water supply and wastewater treatment systems (H.R. 3178, S. 1593). Some of the drinking water research provisions in these bills were included in the Bioterrorism Preparedness Act. In 2002, the House approved a bill authorizing $220 million in grants and other assistance for vulnerability assessments by wastewater treatment utilities (H.R. 5169), but the Senate did not act on a related bill (S. 3037).

In the 108th Congress, legislation authorizing vulnerability assessment grants to wastewater utilities was approved by the House (H.R. 866, identical to H.R. 5169 in the 107th Congress). The Senate Environment and Public Works Committee approved related legislation (S. 1039). No further action occurred, due in part to concerns expressed by some that the legislation did not require that vulnerability assessments be submitted to EPA, as is the case with drinking water assessments required by the 2002 Bioterrorism Preparedness Act.

Wastewater security issues again received some attention in the 109th Congress. In May 2006, the Senate Environment and Public Works Committee approved S. 2781, legislation similar to S. 1039 in the 108th Congress. It would have encouraged wastewater utilities to conduct vulnerability assessments and authorized $220 million to assist utilities with assessments and preparation of site security plans. It also included provisions responding to GAO's March 2006 report that found that utilities have made little effort to address vulnerabilities of collection

[23] These grants, funded at $5 million per year, were discontinued after FY2009 due to completion of states' high priority activities, which consequently decreased demand for the funds, according to EPA.

[24] For information, see CRS Report RL31294, *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions*, by Mary Tiemann.

systems, which may be used by terrorists to introduce hazardous substances or as access points for underground travel to a potential target.[25] S. 2781 would have authorized EPA to conduct research on this topic. During consideration of the bill, the Senate committee rejected an amendment that would have required, rather than encouraged, treatment works to conduct vulnerability assessments and also would have required high-risk facilities to switch from using chlorine and similar hazardous substances to other chemicals that are often referred to as "inherently safer technologies." Similar legislation was introduced in the 110th Congress (S. 1968). In the 111th Congress, H.R. 2883, the Wastewater Treatment Works Security Act of 2009, was introduced to require wastewater utilities that use or store substances of concern to carry out assessments and develop site security plans, in compliance with EPA guidelines. The bill would have authorized $1 billion in grants for vulnerability assessments, security enhancements, or worker training programs. No similar bill was introduced in the 112th Congress.

Another issue of interest has been the concerns of a number of water supply and power users of Bureau of Reclamation facilities about paying for security costs at these facilities. Since 9/11, Reclamation has increased security and anti-terrorist measures at federal multi-purpose dams. From 2002 through 2004, all of the incremental security costs were paid by the federal government. However, since 2005, the Administration has requested that users should fully reimburse government for the guards and patrols portion of site security costs. In the Administration's view, project beneficiaries have had several years to adjust their expectations, budgets, and planning for current guard and patrol levels and that post-9/11 cost increases should now be considered project O&M expenses subject to allocation among project purposes and reimbursement from beneficiaries.

Many users argued that security costs for which the general public is the beneficiary, including obligations for national defense, should properly be the federal government's responsibility. The issue is especially a concern for beneficiaries of Reclamation's five high-priority dams, such as Hoover and Grand Coulee, which have the largest security needs, because these users are being asked to pay a proportionally higher share of total security costs than users of other Reclamation facilities. Hearings on the issue were held by the House Natural Resources Committee, in June 2006, and the Senate Energy and Natural Resources Committee, in July 2007. A compromise on the issue is reflected in legislation enacted in 2008. Section 513 of the Consolidated Natural Resources Act of 2008 (P.L. 110-229) requires water and power users to pay for the cost of security guards, but sets an $18.9 million cap on the amount to be paid by users, indexed for inflation. Since FY2009, Reclamation's budget has included this annual reimbursability ceiling.

Water Utilities and Chemical Plant Security

The issue of security of wastewater and drinking water utilities also was debated in connection with legislation dealing with chemical manufacturing plant security. During consideration of comprehensive chemical plant security bills during the 109th Congress, some proposed that water systems (drinking water and wastewater) be included in the legislation because many store or use extremely hazardous substances, such as chlorine gas, that can injure or kill citizens if the chemicals are suddenly released (see page 4). However, water system officials argued that the water sector should be excluded, because facilities have already undertaken vulnerability assessments (as required for many drinking water systems under the 2002 Bioterrorism Act, and as many wastewater utilities have done voluntarily). Further, they argued that requirements in the

[25] U.S. Government Accountability Office. *Securing Wastewater Facilities, Utilities Have Made Upgrades but Further Improvements to Key System Components May Be Limited by Costs and Other Constraints*, GAO-06-390, March 2006, 64 p.

legislation were potentially duplicative of Risk Management Plan provisions in the Clean Air Act, which apply to more than 2,800 of the largest water systems.

As part of a bill providing FY2007 appropriations for the Department of Homeland Security, Congress included provisions authorizing DHS to establish risk-based and performance-based security standards at the nation's chemical plants (the Chemical Security Act, Section 550 of P.L. 109-295). Under the legislation, chemical plants are required to conduct vulnerability assessment and create and implement site security plans based on identified vulnerabilities. The chemical plant security provisions in P.L. 109-295 agreed to exclude water systems from the new requirements. Implementing regulations were promulgated by DHS in 2007, the Chemical Facility Anti-Terrorism Standards (CFATS). However, under the statute, the temporary DHS rules were scheduled to sunset on September 30, 2009, after three years.[26]

At a House Homeland Security Committee oversight hearing in 2007, DHS Assistant Secretary for Infrastructure Protection Bob Stephan said that the water sector's exclusion from the Chemical Security Act created a "regulatory gap," because chemicals that are covered by the act, including chlorine, are found at unregulated wastewater and drinking water facilities, as well as regulated conventional chemical plants. He also said that DHS is reviewing ways to boost safeguards at water utilities that use large amounts of gaseous chlorine. Similarly, in 2008, EPA and DHS officials testified in support of eliminating the current exemption for wastewater and drinking water facilities from chemical security regulations. Water utilities oppose being included in DHS's CFATS rules, arguing that it could lead to costly new mandates. The debate also has raised the issue of federal agency roles and leadership, such as whether EPA should be granted a formal consultative role in development and implementation of DHS chemical security rules. Some were concerned that legislation would create uncertainty about coordination between EPA and DHS and whether EPA's lead role for the water utility sector would be altered.

Each Congress since the 110th has considered legislation to extend and modify P.L. 109-295, including to make the chemical security standards permanent. Since the CFATS authority in P.L. 109-295 expired in September 2009, Congress has been extending the standards on a year-to-year basis. During this period there have been several competing proposals: to create permanent DHS rules for wastewater and drinking water facilities; or to create permanent DHS security rules for chemical plants and wastewater facilities but exempt drinking water plants; or to require EPA to establish risk-based security rules for drinking water plants and for EPA and DHS to consult on security at co-managed drinking water and wastewater facilities; or to leave the existing exemption in place and designate in statute that EPA is the lead agency for drinking water and wastewater security. Water utilities have urged congressional committees not to create a dual or split regulatory arrangement between two agencies, arguing that EPA has long-standing expertise in water and wastewater security issues.

A controversial issue debated in connection with some of these proposals is whether to require facilities that handle chemicals to take action to reduce the consequences of a terrorist attack, such as using different chemicals, or changing to safer processes for their operations—so-called inherently safer technology (IST). Under some proposals, regulated drinking water and wastewater treatment facilities in high-risk categories could be directed by states or EPA to implement methods to reduce the consequences of a chemical release from an intentional act if doing so is feasible, would significantly reduce risk, would not increase interim storage of a substance of concern at the facility, and would not render the facility unable to comply with applicable requirements of the SDWA or CWA. Supporters have said that including water

[26] For additional information, see CRS Report R41642, *Chemical Facility Security: Issues and Options for the 112th Congress*, by Dana A. Shea

facilities would close a major security gap and would strengthen chemical facility antiterrorism standards and incorporate best practices. Opponents have said that doing so would impose costly mandates while doing little to further security. Water utility officials endorse giving EPA the lead on water security, but oppose any mandate for IST.

Legislative proposals addressing these issues in the 112th Congress included H.R. 901, approved by the House Homeland Security Committee; H.R. 908, approved by the House Energy and Commerce Committee; and S. 473, approved by the Senate Homeland Security and Government Affairs Committee. These bills differed in a number of respects but reflected apparent consensus regarding water utility issues: all of the bills would have preserved the existing exemption from the DHS CFATS program, and none would have mandated inherently safer technology. Further, none would have altered EPA's lead role for the water utility sector. Separate Senate legislation, S. 711, did include provisions to require inherently safer technology and would have added coverage of wastewater and drinking water facilities in CFATS. None of these bills was enacted by the 112th Congress. However, a provision of the Continuing Appropriations Act, 2013 (P.L. 112-175) extended authority for the existing CFATS program through March 27, 2013.

Since the terrorist attacks of 2001, wastewater and drinking water utilities have been engaged in numerous activities to assess potential vulnerabilities and strengthen facility and system protections. Congressional oversight of this sector's homeland security activities has been limited but could be of interest in the 113th Congress.

Author Information

Claudia Copeland
Specialist in Resources and Environmental Policy

Disclaimer